Assurance Cases
for
External Infusion Pumps

Richard Chapman

FDA

May 26, 2010

New External Infusion Pump Guidance

- The new infusion pump guidance steers manufacturers to the top level safety claims based on a comprehensive analysis of the hazards associated with the use of infusion pumps.
- The guidance does this by recommending the use of assurance cases to organize and dictate the content of 510(k) premarket submissions for infusion pumps.

Current system

- Safe and Effective
- 510(k) clearance
  - Substantial Equivalence to a predicate device. This is “Argument by Analogy” – potentially a logical fallacy.

Challenges

- Lack of clear definition of evidence and how to evaluate it.
  - Guidance Documents, Standards
  - Checklist
    - Presence versus quality
  - Domain Experts
- Evidence is:
  - Test data
  - Results from experiments
  - Historical performance
  - Compliance with standards
  - Analysis
  - Scientific and engineering information from the literature

Challenges

- Poor documentation of requirements and environmental assumptions.
  - Hazards
  - System of systems
  - Human Factors
- Infusion Pump
  - Right Drug, Right Person, Right Rate

Challenges

- Incomplete understanding of the appropriate use of inspection, testing and analysis
- No overarching theory of coverage that enables coverage to accumulate across multiple verification techniques.

Standards

- Standards themselves do not provide assurance ….compliance with them can

- Standards must codify attributes which can be objectively assessed in a product by a third party

- Regulators need to regulate products so the attributes of the standard must be evident in the product or its design documentation

This excludes many process standards from being useful to regulators!

‘Software’ standards

IEC 62304

- Requirements for lifecycle processes in software development
- But no requirements for the software itself
  - These processes are **not** quality processes
  - They are in addition to them!
  - They are moderated by the quality processes
  - How do you determine compliance unless you are a developer? Needs deep knowledge of the culture!
  - Hard for a corporate culture to assure itself of compliance!

IEC 60601-1 3rd edition

Clause 14 has software requirements which relate to the product but which are a little difficult to assess

Clause 14.4 refers to development lifecycle and mentions IEC 62304

a) COMPONENTS WITH HIGH-INTEGRITY CHARACTERISTICS;

b) fail-safe functions;

c) redundancy;

d) diversity;

e) partitioning of functionality;

f) defensive design, e.g., limits on potentially hazardous effects by restricting the available output power or by introducing means to limit the travel of actuators.

IEC 60601-1 3rd edition

- The architecture specification shall take into consideration:

g) allocation of RISK CONTROL measures to subsystems and components of the PEMS; NOTE—Subsystems and components include sensors, actuators, PESS, and interfaces.

h) failure modes of components and their effects;

i) common cause failures;

j) systematic failures;

k) test interval duration and diagnostic coverage;

l) maintainability;

m) protection from reasonably foreseeable misuse;

n) the NETWORK/DATA COUPLING specification, if applicable.

- Requires mandatory compliance with ISO 14971 standard for risk management processes

Ah Hah!

- So here we have some concrete examples of implementation which a third party can observe to assure safe and effective product.
- Q. But how do we know whether the design implementation decisions were ‘well made’?
  - ‘Well’ made in the sense of;
    - Good technical judgment was applied
    - Correct trade-offs used in the design
    - Correct balance in the trade-offs
    - Competently implemented in the design
    - Properly manufactured to reflect those trade-offs
- A. Risk management tells us

So what do premarket technical regulators really look for?

What the design trade-offs actually were:

- Are they safe?
- Who made them and stands by them?
- Why they were made this way?
- How they were verified as the right ones?
- Can they be reeled back if something goes wrong later?
- Are they at or near the currently accepted state of the art?
- Can manufacturing realize the product once approved with the same trade-offs?
- Will they persist in continued use?

These trade-offs manifest as

- Requirements translated into specifications
- Standards translated into controls
- Manufacturing translated into products
- Manufacturing controls translated into Quality systems which tend to comply

Did you see any process standards there?

- Probably not…..
- These things are the decisions made by real engineers every day
  - They don’t have to be perfect (that’s the law!)
  - Just good enough!
  - … and transparent to the regulator
- There is no process standard for good decisions!

Risk management

Lets look at software.

- What are the ways in which the software might fail in use?
  - 'Hazardous situations' which we have not anticipated e.g.
    - Keys pressed too quickly (I/O buffer size too small)
    - Metrology errors (defective algorithm)
    - Logic errors (if..elseif…elseif..endif..oops)
    - Semantic errors (casting a long into a short)
- Compilers may not (usually not) catch these things
- Industry has traditionally relied on the marketplace to inform us of these bugs.
- Not good enough anymore in this industry!

How to avoid these types of problems?

- Simulation
  - User interactions
  - State machine modeling & analysis
- Design for verification
  - Restricted syntax rules
- Static analysis
  - Automated traverses of the call graph
- Experienced engineers

Can auditing help?

- Yes….provided its technical. This proposed type of self assessment differs markedly from QMS auditing in that highly skilled technical resources with experience can expose these types of problems.
  - Could be expensive if contracted out…
  - IP issues, time to market issues
- Auditing quality processes won't help because the trade-offs (the ones we're often sorry we made) are often 'underneath' the QMS control layer.

So how can a manufacturer maximize compliance in a QMS?

1. Recognize that QMS do not usually expose a bad decision, or a bad design but, when overly burdensome, can often hide these mistakes!
2. Recognize that the Quality management process is **necessary** but **not sufficient** on its own. It is there to ensure ongoing compliance after initial approval. The engineering itself must be accessible for the premarket review. A convincing argument must be made as to why this engineering approach is sufficient.

So how can a manufacturer maximize compliance in a QMS?

3. Incorporate risk management processes into the QMS.
4. Prepare design documents which explain why choices were made in that way. It will explain why the requirements have changed during the development life-cycle. It might even be part of the requirements documentation itself. Legally marketed devices don’t have to be perfect.

One possible answer

- A Safety Assurance Framework
- A process for distilling the reasons for product integrity from the totality of activities and resources employed to realize it.
- … and for making an argument as to why the evidence, your data and analyses, supports the claims

How does this relate to FDA premarket processes

- A 510(k) is mostly a checklist
- FDA asserts that we know what we want
- Sponsor just follows the checklist
- Once upon a time a checklist was a way to assure coverage and completion and equitable application
- As systems become more complex this becomes less true

- With increased functional complexity comes increased diversity of solutions. With increased diversity of solutions comes diverse implementations and our equitable review begins to become harder

- We soon don’t know what to ask for, so we rely on additional information requests to satisfy coverage, but this consumes time so we begin to take a risk management approach

- A safety case is the best way to both document and review a submittal based on a risk management approach because the argument shows the proportionality of the mitigation

Where did this all come from?

- Stephen Toulmin a professor of philosophy and mathematics at Oxford in 1949 wanted to examine the mathematical formalisms of argument and certainty.
- Wrote several books which did not sell!
- But which, surprisingly, are used today as teaching aids to litigators, safety professionals, regulators, scientists, and intelligence communities.

Reasoning

- **Legal system**
  - Risk based
    - Reasonable suspicion – temporary loss of liberty
    - Probable cause – arrest
    - Beyond a reasonable doubt – Loss of life or liberty
    - Civil court – preponderance of evidence – loss of money
- **Scientific Method**
  - Hypothesis
  - Experiments, methods, to test the hypothesis
  - Statistical measures of the reliability of data
  - Discussion and conclusions

The assurance case is a method for reasoning about systems appropriate for scientists and engineers.

What does this mean?

- Generalized Assurance Case
  - – Safety case
  - – Compliance case
  - – Effectiveness case
  - – Business case
  - – ….

What is a Safety Case?

A structured *argument*, supported by a body of *evidence*, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment

- This type of assurance case contains a structured argument (rationale) demonstrating that the evidence it contains is sufficient to show that the system is safe
- The argument is commensurate with the potential risk and the system’s complexity

Hazard Analysis

- Start with the hazards
- The claim is that you have mitigated the hazard or the hazardous situation.
- Determine the properties of the system that will make it safe.
- Generate safety requirements

Evidence

- There are three types of evidence, with respect to safety requirements, that are necessary for a complete safety argument:
  - **Requirements Validation** - Demonstration that the set of Safety Requirements is complete and accurate
  - **Requirements Satisfaction** - Demonstration that all Safety Requirements have been met
  - **Requirements Traceability** - Demonstration that all Safety Requirements have been tracked throughout all stages of System Development and Safety Analysis

Evidence

- At the system level, evidence must be provided for each of these categories. If the set of identified system safety requirements can be shown to be valid, satisfied and traceable, then it can be argued that the system is acceptably safe.

- Evidence is:
  - Test data
  - Results from experiments
  - Historical performance
  - Compliance with standards
  - Analysis, and
  - Scientific and engineering information from the literature

Suitability of Evidence

Assurance (of a Requirement for Evidence) The degree of confidence that the set of safety evidence satisfies the requirement for evidence.

- **Relevance -** The extent to which an item of evidence entails the requirement for evidence
- **Trustworthiness -** The perceived ability to rely on the character, ability, strength or truth of the evidence
- **Independence -** The extent to which complementary items of evidence follow diverse approaches in fulfilling the requirement for evidence

Suitability of Evidence

Relevance - The extent to which an item of evidence entails the requirement for evidence

- **Directness -** The extent to which an item of evidence directly fulfils the requirement for evidence
  - Direct – e.g., timing data
  - Indirect – e.g., competence of personnel
- **Coverage -** The proportion of the requirement for evidence which the evidence addresses
  - Thorough – e.g., a technique which provides evidence of the handling of all runtime exceptions
  - Less thorough – e.g., a technique which provides evidence of the handling of divide by zero

Suitability of Evidence

Trustworthiness - The perceived ability to rely on the character, ability, strength or truth of the evidence

- The trustworthiness of evidence is an expression of the ***process evidence*** related to generating the evidence. These factors include, but are not limited to:
  - "Buggy-ness" – how many "faults" there are in the evidence presented;
  - Level of review;
  - For tool-derived evidence: Tool Qualification and Assurance;
  - Experience and Competence of the personnel.

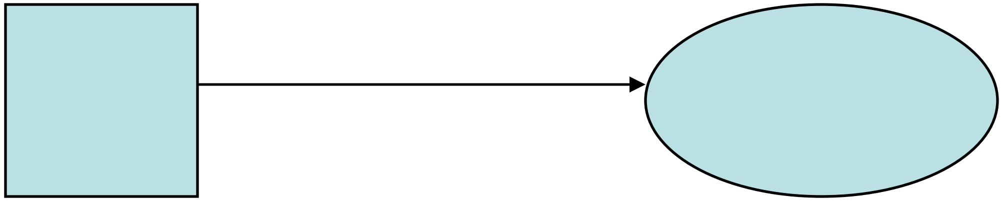
Suitability of Evidence

Independence - The extent to which complementary items of evidence follow diverse approaches in fulfilling the requirement for evidence

- Independent - Manual code inspection and static analysis are independent methods to eliminate software defects
- Not Independent - Human factors testing by software developers is the fox watching the hen-house

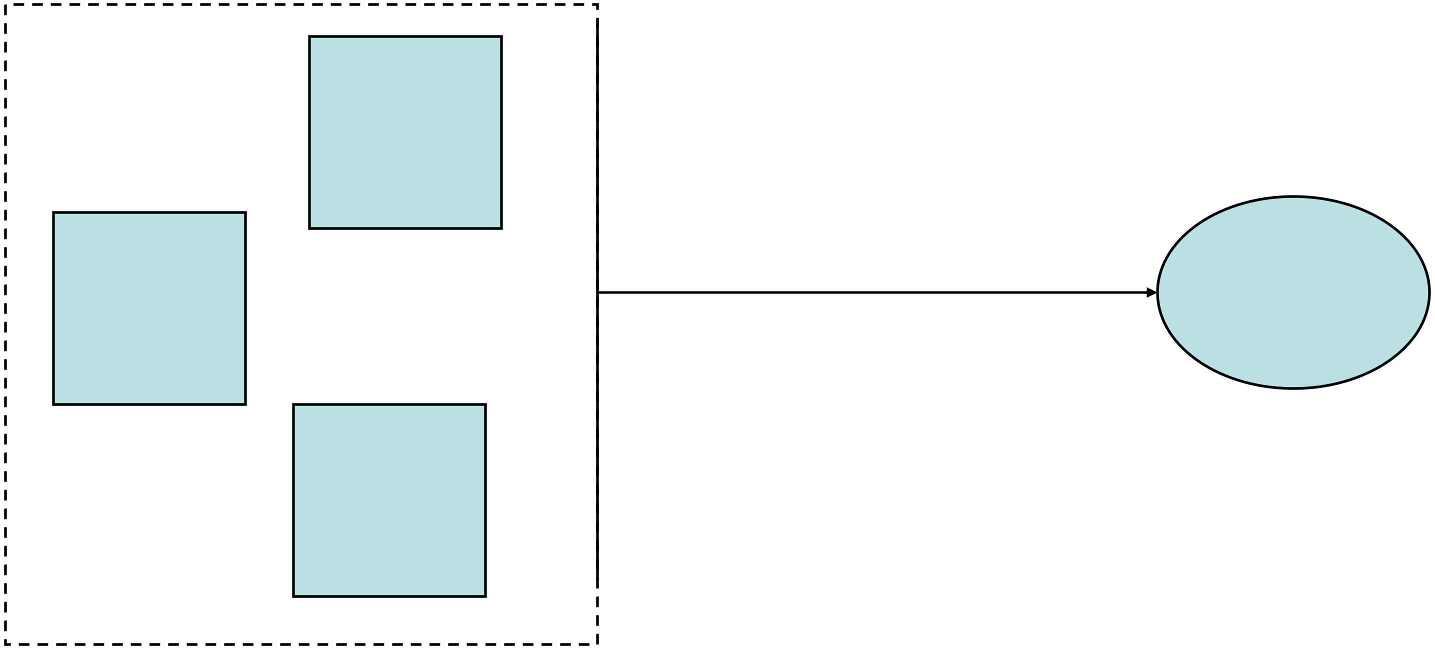
Support Patterns

- Single Support Pattern
  - One premise supports the conclusion



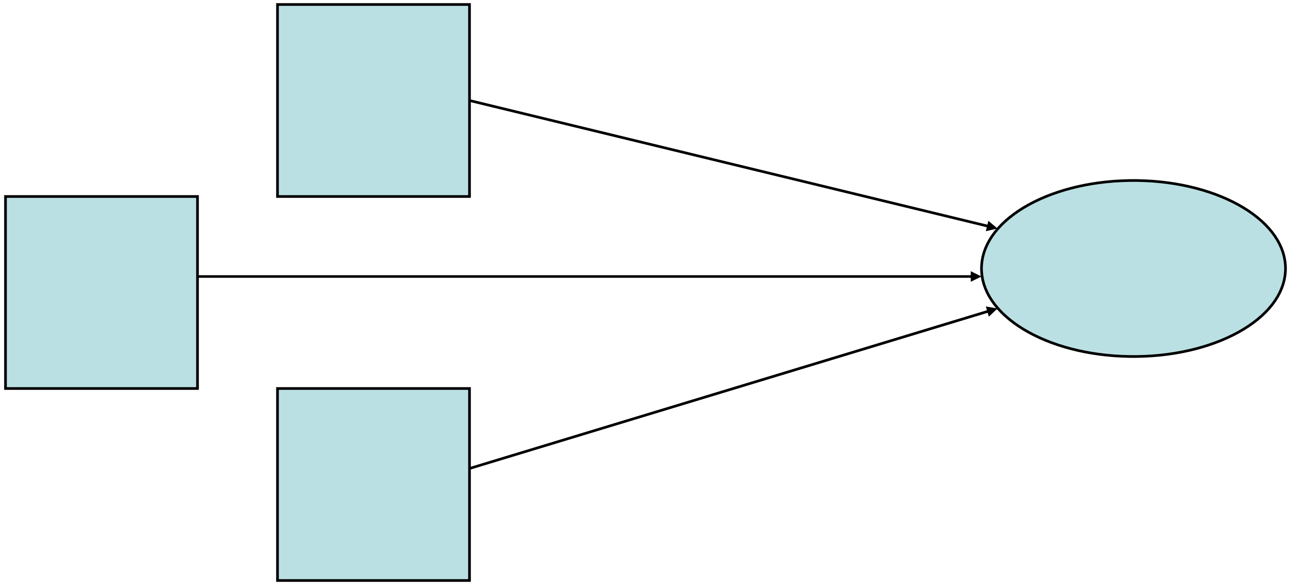
Support Patterns

- Linked Support Pattern
  - Several premises interdependently support the conclusion



Support Patterns

- Convergent Support Pattern
  - Several premises each separately support the conclusion



Argumentation

The action or operation of inferring a conclusion from propositions premised.

- **Premise -** A previous statement or proposition from which another is inferred or follows as a conclusion

Argumentation

- **Conclusion -** A judgment or statement arrived at by any reasoning process
  - Deductive - If premises are true, then the conclusion must also be true
  - Inductive - The conclusion follows from the premises not with necessity but only with probability
  - Abductive - Inference to the best explanation
  - Argument by Analogy

  - Beware of logical fallacies
    - Argument by analogy
    - Drawing the wrong conclusion
    - Omission of key data
    - Etc.

Argumentation

- The strongest arguments are both valid and sound
  - **Valid** - If premises are true, conclusion is true
  - **Sound** - Argument which is valid and has true premises
- Weaker Argument
  - **Consistent -** If premises are true, conclusion may be true. True with some probability.

What is a Safety Argument

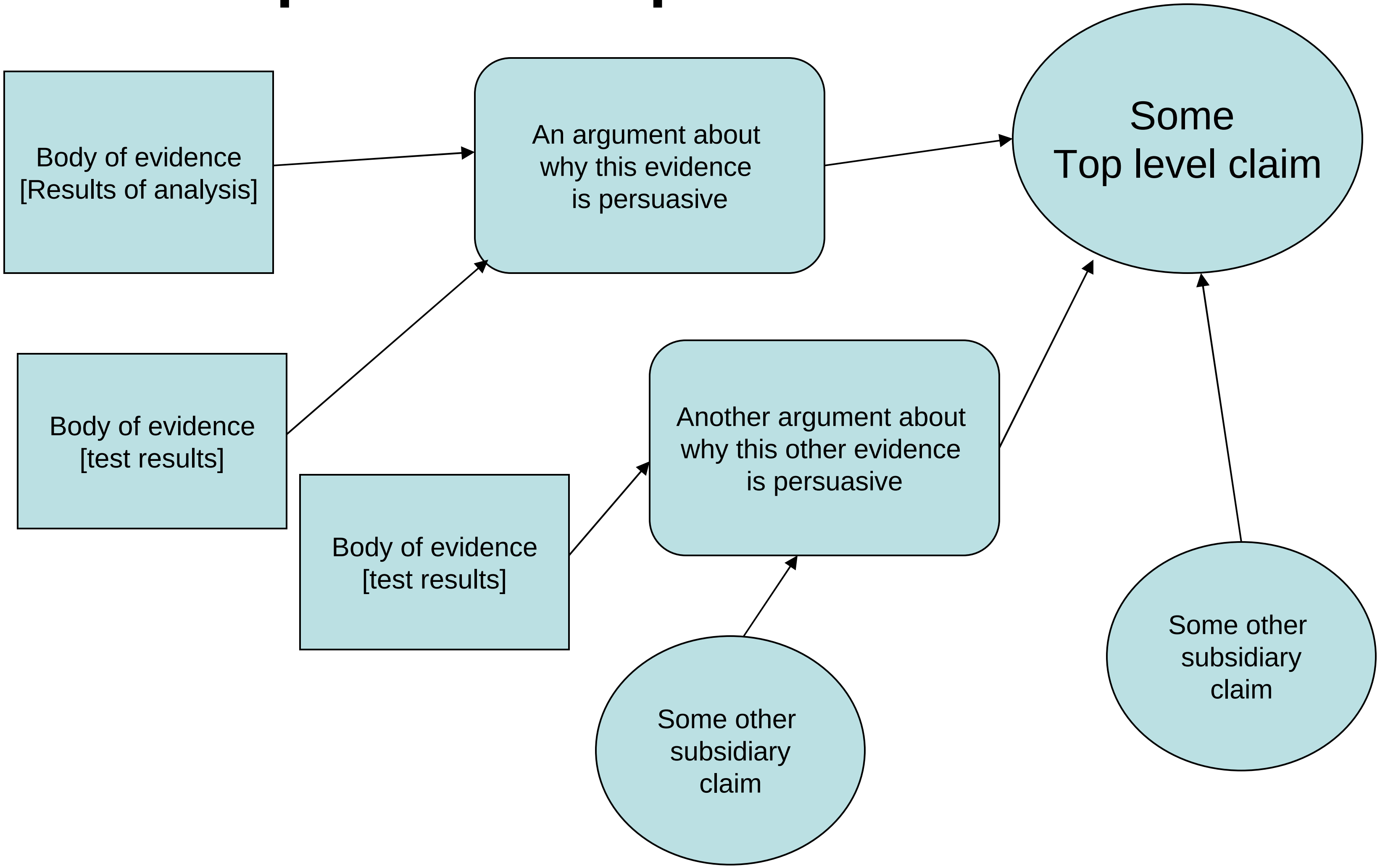
- **This infusion pump is safe because**
  - **The safety requirements are defined in my**
    - **Safety requirements analysis, derived requirements ...**
    - **Legislation, policy …**
- **The safety requirements are met through our**
  - **Safety analysis of design, use …**
  - **Hazard management through problem reporting**
  - **Observing failures are at a ‘safe’ level**
  - **Appropriate quantity, quality and rigor of evidence**
- **Safety management continues to be adequate because we have**
  - **SMS**
  - **staff competence**
  - **ongoing independent scrutiny ...**

Format

- Narrative
- Tabular
- Graphical

- All are acceptable formats
- Tools
  - Adelard – ASCE
  - Will implement others that manufacturers choose to use

Graphical representation



Body of evidence
[Results of analysis]

Body of evidence
[test results]

Body of evidence
[test results]

An argument about
why this evidence
is persuasive

Another argument about
why this other evidence
is persuasive

Some
Top level claim

Some other
subsidiary
claim

Some other
subsidiary
claim

Logical schema

- Each claim;
  - must have at least 1 child argument
  - can have zero or more subsidiary child claims
  - must have no child evidence
- Each argument
  - Must have one or more parent claims
  - Must have one or more child evidence
  - Can have zero or more child claims
- Each bit of evidence
  - must have one or more parent arguments
  - must have no child evidence, child claims or child arguments

Such a data structure has interesting properties!

- It can be proved!
  - Checked (automatically) to verify logical completeness, structural correctness
- It can be recursed
  - Lends itself to system engineering principles
  - Delegation of tasks
  - Hiding of properties
  - Weighting of assurance levels

- It can be exported
  - Many components and accessories can be rolled-up into an overall system assurance case
- It can be displayed graphically to provide the ‘big picture’

Safety Case Reports

- **The Safety Case**
  - A complex body of interdependent and evolving documentation
  - Created and managed by the manufacturer
  - Not easily auditable or reviewable

- **Safety Case Reports**
  - A ‘snapshot’ of the rationale and content of a safety case at an appropriate milestone
  - Shows that any arbitrary set of requirements has been met

Safety Case Reports

- Safety Case Reports (continued)
  - Reviewable against the project expectation at the milestone
  - May need several report types for various stakeholders
  - May need several updates over time

Who reviews such a report?

- Primarily the manufacturer
  - To show management that certain criteria have been met
  - To minimize effort while demonstrating compliance
- Secondarily a third party, consultant or customer
  - Can develop the evidence (e.g. test house)
  - Can audit the compliance (QMS registration, CE marking, Purchase specs)
- Finally the regulator
  - Knows already what the claims are!
  - Can see the evidence anytime
  - But does want to know, premarket, how persuasive the arguments are

Implications for manufacturers

- The Safety Case will evolve over the life of the system
- While the structure of the Safety Case will broadly remain constant,
  - the status of the evidence will change, e.g., planned test coverage will be replaced by evidence of test results
  - the relative weight of the arguments may change, e.g., compliance with a process standard might be replaced by proven in use
- Therefore plan for multiple reports
  - Obtain agreement on the argument structure first
  - Use identification of evidence as management tool

Examples

- Charles B. Weinstock, John B. Goodenough. 2009. Towards an Assurance Case Practice for Medical Devices. SEI **TECHNICAL NOTE** CMU/SEI-2009-TN-018
  - Infusion pump specific
  - **http://www.sei.cmu.edu/reports/09tn018.pdf**

Thank You!

Questions?